العنوان: جرائم الحاسوب وأساليب مواجهتها
المصدر: الأمن والحياة (أكاديمية نايف العربية للعلوم الأمنية) - السعودية
المؤلف الرئيسي: أبكر، سليمان مصطفى
المجلد/العدد: مج 19, ع 210
محكمة: لا
التاريخ الميلادي: 2000
الشهر: ذوالقعدة / مارس
الصفحات: 48 - 50
رقم MD: 309387
نوع المحتوى: بحوث ومقالات
قواعد المعلومات: HumanIndex
مواضيع: الجريمة و المجرمون، الحاسبات الإلكترونية، جرائم الحاسبات الإلكترونية، أساليب المواجهة، التخطيط الأمني، الإستراتيجيات الأمنية، سرقة الأموال النقدية، السطو الفيروسي ، سرقة البرامج، أمن المعلومات
رابط: http://search.mandumah.com/Record/309387

جرائم الحاسوب وأساليب مواجهتها

مقدم سليمان مصطفى أبكر*

عندما نتحدث عن الحاسوب أو الحاسب الآلي أو الكمبيوتر نعني بذلك جهاز الكمبيوتر من حيث النواحي المادية Wardware والنواحي غير المادية Software ونلاحظ أن الحاسوب من الأجهزة التي يجري عليها الإحلال والتطوير بشكل متسارع الخطى في عالم التقنية.. ونجد أن تطور الجريمة بذات التسارع في كثير من الدول، رغم الضمانات الفنية والتقنية تعرض الحاسب الآلي إلى أكثر من مرة لاختراق تأمينه ولم يكتف المجرمون والمحترفون في هذا المجال بسرقة الأجزاء المادية Hardware وسرقة البرامج Software والمعلومات والبيانات Information أو سرقة الأموال باستخدام الحاسوب ولكن امتد الإجرام إلى اختراق الشبكات العسكرية واستراتيجيات القومية وتأثير ذلك في حالة الاستعدادات العسكرية وتنفيذ الخطط والبرامج السرية للدول والشركات والمؤسسات.

ويمكن تعريف جريمة الحاسوب بأنها الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة ومصلحة الأفراد (خاصة).

ومن أمثلة هذه الجرائم سرقة الأموال النقدية والسلع والبرامج والبيانات وتدمير البيانات أو ملفات محددة واختراق الشبكات وكشف المعلومات أو الأسرار أو استغلال وقت الحاسوب بشكل غير قانوني ودائماً محترفي جرائم الحاسوب من الذين لهم دراية بالنواحي الفنية عن الحاسوب

وتكلف خسائر جرائم الحاسوب مبالغ طائلة جداً وقد قدرت الخسائر في الولايات المتحدة بخمسة ملايين دولار سنوياً وقد قدرت المباحث الفيدرالية الأمريكية .F.B.I في نهاية الثمانينيات أن جريمة الحاسوب الواحدة تكلف ٦٠٠ ألف دولار سنوياً وفق دراسة أجراها أحد مكاتب المحاسبة الأمريكية منها ٢٤٠ شركة أمريكية وقعت ضحية جرائم الغش باستخدام الحاسوب Computer Frand وفي دراسة أجريت في المملكة المتحدة ثبت أن ما يقارب ٢١٢ جريمة من جرائم الحاسوب قد تم ارتكابها وأكثر هذه الجرائم نتجت عن سوء استخدام البرامج التي تنفذ الإجراءات المطلوبة باستخدام الحاسوب أو إلى سوء تغذية الأجهزة ببيانات غير صحيحة.

ويمكن تقسيم جرائم الحاسوب إلى خمس مجموعات:

- المجموعة الأولى: تشمل الجرائم التي تتمثل في اختراق الحاسوب لتدمير البرامج والبيانات الموجودة في الملفات المخزنة بالحاسوب وهذه هي من أخطر أنواع الجرائم، وهنا يقوم شخص متخصص بوضع أمر معين Command لبرامج الحاسوب، وعند تنفيذ هذا الأمر يتم مسح كلي أو جزئي للملفات المرتبطة بهذه البرامج ويتم هذا النوع من الجرائم بصورة متعمدة.

- المجموعة الثانية: وتتمثل في الجرائم

التي يتم بها استغلال البيانات المخزنة على الحاسوب بشكل غير قانوني ومن أمثلتها الدخول إلى شبكة الحاسوب التي تحمل أرقاماً سرية محددة من خلال استخدام الحاسوب للحصول على مبالغ نقدية تحت هذا الرقم أو الاختراق لكشف الأسرار أو لأغراض أخرى.

ـ المجموعة الثالثة: تشمل الجرائم التي تتم باستخدام الحاسوب لارتكاب جريمة معينة أو التخطيط لها.

ـ المجموعة الرابعة: وتشمل الجرائم التي يتم استخدام الحاسوب بشكل غير قانوني من قبل الأفراد المخصص لهم باستخدامه ومن أمثلة ذلك استخدام الموظفين أو العاملين بمركز الحاسوب للأجهزة بعد أوقات العمل الرسمية أو أثناءه مثل استخدامه في التسلية ببرامج الألعاب أو بعض الأغراض الشخصية غير المرتبطة بالعمل الرسمي أو الاستخدام العشوائي لمفاتيح الأوامر من الذين لا يجيدون استخدام الحاسوب.

ـ المجموعة الخامسة : وتتمثل في فيروسات الكمبيوتر والفيروس ما هو إلاّ برنامج آخر موجود على الكمبيوتر يهدف إلى إصابة الكمبيوتر لإتلاف البرامج وربما كان السبب في ازدياد الرعب من الفيروس هو التزايد الهائل في حجم الاعتماد على أجهزة الكمبيوتر وشبكاتها والخدمات العامة التي توفرها مراكز الحاسوب بالمصالح العامة والخاصة ودائما ينتقل الفيروس عند استخدام وسيط تخزيني ملوث بفيروس من الفيروسات Storage Media وعند إدخال الوسيط وتحميل البيانات Loading Data على الحاسوب يتم تدمير البيانات أو تعطيل استخدام البرامج الأصلية المخزنة على الحاسوب وقد يتصادف إرسال مجموعة أسطوانات من جهة بالبريد ويكتشف بأن تكون ملوثة بفيروس لذا يفضل تجربة هذه البيانات قبل تخزينها على الحاسوب الرئيسي وبعض الفيروسات موجود أصلاً بالجهاز ولكن تنشط من وقت لآخر عند تنفيذ بعض الأوامر أو الألعاب.

وبوجه عام تتقاسم كل الفيروسات الصفات الآتية:

ـ خاصية التسلل والعمل في الخفاء Stealth.

ـ خاصية التكاثر Riplication ويعني بأن يصيب الفيروس جهاز الكمبيوتر ويقوم بنسخ نفسه عدة مرات بهدف الانتشار والالتصاق في الملفات المتناثرة على الأسطوانة.

ـ خاصية التخزين في برامج بدء التشغيل Boot Sector وهذه الفيروسات الذكية تقوم بنسخ نفسها في جزء من الأسطوانة المخصصة لتخزين برامج بدء التشغيل لتسهيل فرص الإصابة وبعضها يتكاثر في الذاكرة Ram.

ـ ويمكن تحديد الجناة (مرتكبي جرائم الحاسوب) إلى خمس مجموعات رئيسة:

١ ـ الموظفون الساخطون على مؤسساتهم الذين يعودون لمواقع العمل بعد فترات العمل الرسمية إما لغرض سرقة المعلومات أو بغرض التخريب.



٢ ـ الموظفون العاملون بمراكز الحاسوب وهؤلاء يمثلون الغالبية العظمى من مرتكبي جرائم الحاسوب وذلك لسهولة اتصالهم بالحاسوب.

٣ ـ فئة العابثين Hachers هم الذين ليس لديهم سلطة استخدام الحاسوب ولكنهم مغرمون بالعبث وهم يستخدمون الحاسوب من أجل التسلية وليس بغرض التخزين وغالباً ما يكونون من هواة الكمبيوتر.

٤ ـ الفئة التي تعمل في مجال الجريمة المنظمة باستخدام الحاسوب حيث يقوم هؤلاء باستخدام الحاسوب في شكل غير قانوني في معرفة بعض الأشياء المتعلقة بالأساليب الأمنية المتبعة لتأمين المؤسسات التي يسطون عليها.

٥ ـ فئة صانعي وناشري الفيروسات Siluation of Computer Criminal Viruses.

ويتم ارتكاب جرائم الحاسوب في المراحل التالية:

ـ مرحلة إدخال البيانات: مرحلة تشغيل البيانات، ومرحلة إخراج البيانات. وبالنسبة لمرحلة إدخال البيانات تحدث لجريمة إذا قام المستخدم بتزوير أو تغيير (فبركة) البيانات ومثال ذلك إذا استطاع الجاني الوصول إلى البيانات المتعلقة بفاتورة الهاتف قبل إعدادها بشكلها النهائي من قبل شركة الهاتف وتمكن من حذف بعض المكالمات من القاتورة قبل إرسالها بالبريد أو أثناء قيام أحد مدخلي البيانات بتغيير الإجراءات أو المستندات الثبوتية لشخص ما أو قام الجاني بتغيير معلومات شخص مشتبه (محظور).

ـ مرحلة تشغيل البيانات :مرتكبي هذه الجرائم يقومون بتعديل البرامج الجاهزة Software التي تقوم بتشغيل

البيانات للوصول إلى البيانات نتائج محددة أو مقصودة من قبل الجاني وفي هذه الحالة يجب أن يكون الجاني على قدر من الدراية والمعرفة بالنظام (مبرمج أنظمة).

- مرحلة إخراج البيانات : وهي أكثر المراحل التي تنتشر فيها جريمة الحاسوب وتتم في هذه المرحلة سرقة المعلومات أو البيانات المتعلقة بالرقابة على المخزون في إحدى المصالح أو إفشاء بعض المعلومات الخاصة بالإجراءات الأمنية الخاضعة للفحص السري لتأمين وضع معين عند موقف معين عند السلطات العسكرية أو أي معلومات بالوزارات أو بالشركات أو الأفراد.

أساليب تلافي جرائم الحاسوب Compute Security:

تتراوح أنواع الحماية من مجرد إحكام إقفال الأماكن التي يوجد بها الحاسوب إلى مجموعة من الطرق التي تستخدم لتكويد (تشفير) البيانات بطريقة لا تمكن الآخرين من اختراق شبكاته وقراءة بياناته والدخول إليها والتلاعب بها.

- وبما أن الحاسوب يشتمل على جانبين مادي Hardware وغير مادي Software فإن سبل الحماية يمكن تقسيمها إلى أمان مادي لمكونات الأجهزة وأمان غير مادي للبيانات والبرامج Brograms and Datas ويتمثل الأمان المادي في حماية مكونات الحاسوب المادية من أخطار القوى الطبيعية ومن الأخطار الناجمة عن تصرفات الإنسان Man-Made -Damage ويمكن تحقيق التأمين المادي من خلال:

- وضع مجموعة من الإجراءات والضوابط تمنع الأفراد غير المصرح لهم باستعمال الحاسوب من دخول مراكز الحاسوب بحيث يوضع الحاسوب الرئيسي في حالة الشبكات Main Frame أو الـ File Server في مواقع تحميه من الهجوم المادي والتحكم في الدخول إلى أماكن وجوده ومن أدق سبل ضبط الدخول والخروج لمراكز الحاسوب. استخراج البصمات الصوتية وبصمات الأصابع للأشخاص المصرح لهم بالدخول أو استعمال شبكية العين Retina وتتم مضاهاتها مع الشخص المدخل باستخدام وسائل آلية سريعة.

- حماية برامج الحاسوب بعمل نسخ احتياطية من البرامج باستخدام الوسائل التخزينية التي تحفظ البرامج والملفات المختلفة لاستخدامها في حالات تلف وسائط التخزين الأصلية أو حدوث أي حذف من أجزاء البرامج أو كلها.

- إحكام أقفال الأمان التي يوجد بها الحاسوب.

- حماية الحاسوب من النيران وأخطار المياه والرياح والحرارة.

وتختلف أساليب مواجهة جرائم البرامج والبيانات بعض الشيء عن أساليب مواجهة جرائم الجزء المادي لأنه من المنطقي أن يظل الحاسوب متاحاً لمستخدميه معظم الوقت إن لم يكن طوال الوقت، وعليه فمن الضروري حماية البرامج الجاهزة Software والمعلومات أو البيانات Informations of Datas ضد الجرائم المختلفة ومع التطور السريع في صناعة الحاسبات والبرامج الجاهزة والوسائط التخزينية المتوفرة بكم هائل من البيانات والمعلومات التي يتم تداولها من خلال مراكز الحاسوب وتداول البيانات من خلال الإنترنت Internet وسهولة اتصال الحاسبات ببعضها البعض سواء في شكل شبكات محلية Local Area Network (LAN) أو شبكات واسطة Wide Area Network (WAN)) فإن مشكلة أمن وحماية البيانات تزداد صعوبة وتعقيداً.

ومن أنسب السبل والوسائل لحماية البيانات (شفرة) للاتصال والدخول إلى الحاسوب Access Code مثل استخدام الأرقام التي تعطيها البنوك للعملاء والشركات لمستخدميها عند سحب الأموال من حساباتهم بنظام بطاقات الائتمان المغنطة والبطاقات التي يتم استخدامها لحساب وقف استخدام الحاسوب من قبل الأفراد حتى يمكن تحاشي سرقة الأموال ووقف الحاسوب.

- استخدام كلمة مرور Pass Word أو كلمة السر وهي عبارة عن كلمة أو عدة أرقام تتم تغذية الحاسب الآلي بها ولا يعرفها إلاّ مستخدمها.

أمن المعلومات في الحاسب الآلي:

نعني بأمن المعلومات في الحاسب الآلي حماية المعلومات من الاطلاع عليها بواسطة الأشخاص غير المأذون لهم وتأمين هذه المعلومات للتعامل معها بواسطة الأشخاص المأذون لهم متى ما أرادوا! إن طرق مراجعة البيانات والحماية المعقدة وبرامج الحاسب الآلي التخزينية والأمنية وقوانين الدول لا تستطيع وحدها تأمين المعلومات في الحاسب الآلي وأن مُثل وأخلاق وأمانة العاملين في حقل الحاسب الآلي وضماناتهم على الأنظمة التي يتعاملون بها من أهم عوامل ومؤثرات تأمين المعلومات وعلى كل العاملين بالحاسبات الآلية مراجعة الالتزام بأخلاق المهنة من حين لآخر.

* الإدارة العامة للجوازات والجنسية - الخرطوم